

UK EMPLOYEE PRIVACY NOTICE

(Applicable to all UK Team Members)

ABM Aviation UK Limited, ABM Facility Services UK Limited, ABM Technical Solutions Limited and ABM Critical Solutions Limited.

This Employee Privacy Notice explains how your employer, one of the companies listed above, handles and uses personal data collected about you.

“We” or “our” or “us” means the companies listed above that employs you. You may contact us about this notice by emailing our representative, Susan Mason, at Susan.Mason@abm.com or emailing UKprivacyquestions@abm.com.

“You” or “your” means our current and former employees (team members), job applicants, consultants, individual contractors, and third parties whose information is provided to us in connection with the employment or other working relationship (e.g., we may be provided with emergency contact information and/or information about dependents).

We are committed to protecting your personal information and to being transparent about what information we hold. Your personal data will be treated in a secure and confidential manner and only as explained below, or otherwise explained to you in writing. Our procedures are governed by the UK General Data Protection Regulation (UK GDPR).

This notice informs you about how we handle and collect your personal data. Please read it carefully.

What Information About You Do We Collect?

We collect and keep information that can be used to identify you or is related to your identity. This information includes:

- Personal details, such as your name, gender, nationality and marital status
- Recruitment information, such as skills, experience, qualifications and references
- Payroll and benefits information, such as amount of pay, overtime, bonus details (if applicable) and bank account details, names and birth dates and National Insurance Numbers of dependents
- Time and attendance records, such clock in / clock out information, and leave / absence records
- Performance information, such as manager feedback and performance reviews
- Health and safety information, such as audits, screening requests, incident reports and risk assessments
- Human Resources information, such as personnel number, payroll number and job title

- Training information, such as records concerning training needs or whether you have completed training
- Disciplinary records, such as complaints and records of investigations
- Computer use, if allowed by law, we may monitor how our computers are used by you, including websites you visit
- Identification checks, such as results of criminal checks and Right to Work (RTW) verifications, Health, safety, and welfare, such as occupational health information, disabilities or details about special requirements
- Financial information, such as benefits data, pay deductions owed to third parties and bank account information
- Photographs or videos, as needed to identify you
- Location data, such as vehicle location and time clock check-in location

We may also collect other information which you choose to provide us during the course of employment.

You may also provide us with information about other people, like your dependents and family members, so that we can provide benefits or contact someone in an emergency. Before you provide data to us about other people, you should inform them of the information which you intend to provide to us. If you share their data with us, they may wish to read this notice, as well.

If allowed by law or with your consent, we may also collect certain information called “sensitive personal data”. This means information such as:

- Race or ethnicity
- Medical information
- Fingerprints (used in connection with timeclocks or IT device logins)
- Religious or philosophical beliefs
- Physical or mental health
- Trade Union membership
- Sexual orientation
- Criminal records and information regarding criminal offences

How Do We Collect Your Information?

We may collect your personal data from more than one place, but mainly directly from you. You will usually provide this information directly to your managers or local HR contact or directly into our HR system Team Member Gateway (TMG). We also collect your personal data from your managers, HR, or co-team members (for example, manager feedback).

We may collect personal data from a previous employer, doctors, Tax and National Insurance authorities, benefit providers or where we employ another party to carry out a pre-employment background check (where allowed by law). This information includes:

- Personal details, such as name, gender, nationality and marital status
- Recruitment information, such as skills, experience and qualifications
- Identification checks, such as results of criminal checks and Right to Work verifications
- Health, safety and welfare, such as occupational health information, disabilities or details about special requirements
- Financial information, such as benefits data, pay deductions owed to third parties and bank account information

Why Do We Collect Your Information?

Whenever we collect your personal data, we do so because there is a legal reason or other need. Most of the time, we collect your information because:

- We need to meet our legal obligations; or
- You signed an agreement (including electronic agreement) which requires us to collect your information, or give your information to another party, or we need to take steps at your request prior to you entering into such an agreement; or
- Collection is for a legitimate interest.

Where we collect data for our legitimate interest, it is usually because we have an interest in attracting and hiring qualified employees, preventing fraud and managing our business. This is important so that we meet our customers' expectations, legal obligations and other business needs. Sometimes, we will collect and provide your personal data to another party like a customer because we have been asked to do so (for example, to meet the security requirements of our customers). We will not collect or provide your personal information when the need to do so is overridden by your interests or fundamental rights and freedoms.

In some cases, you may ask us to provide your information to another party for a special reason, and we will follow your instructions on your behalf (for example, if you ask us to provide pay information to a bank for a mortgage application made by you).

When we collect sensitive personal data, it is for the reasons above and because:

- We need to meet our obligations and to exercise your rights or our rights under employment law, social security law and social protection law; or
- We need to determine whether you can work, or to provide health or social care or treatment or the management of health or social care and services; or
- We need to protect your vital interests or the interests of another person where you are physically or legally not able to give consent (for example, in a medical emergency); or
- We want to ensure equality of opportunity or treatment between people of different racial or ethnic origins, people with different religious or philosophical beliefs, people with different states of physical or mental health or people of different sexual orientation.

We may also collect information about criminal convictions and offences if allowed by law. For example:

- a criminal record check during recruitment or transfer or where ongoing screening is required because you have applied to work in a role where a check is allowed by law;
- an allegation of a criminal offence or conviction arising during your relationship with us will be processed (e.g., in a disciplinary process) so that we can make decisions about your relationship with us.

If you would like more detailed information about the lawful basis of processing, please email UKprivacyquestions@abm.com.

Do We Need Your Consent?

We may sometimes ask for your consent to collect and use certain kinds of information when there may not be a legal or other reason to collect this information. The reason for doing so will be provided to you at the time we ask for your voluntary consent. It is not a condition or requirement of your employment to agree to any request for consent from us.

How Long Do We Keep Your Information?

We will keep your information only for as long as we need to. The amount of time we need to keep your information will depend on the nature of the information. You may view our schedule for deleting your information by contacting us at UKprivacyquestions@abm.com.

Who Do We Share Your Information With?

Your information will be shared with the members of our HR team and management who are responsible for making decisions about your relationship with us, in addition to other departments which need your information to meet certain requirements.

We may also provide your personal data to another party like a customer because we have been asked to do so (for example, to meet the security requirements of our customers). Some of your information will also be shared with organisations or other companies that provide services to us, such as our payroll provider who issues your pay. These companies or organisations will change from time to time. Examples include Tax, National Insurance, and social security authorities, regulatory authorities, our insurers, bankers, IT administrators, lawyers, auditors, investors, health and safety consultants, recruitment agents, occupational health providers and other professional advisors, HR system providers, payroll providers, benefit providers and administrators, third party staff vetting providers and medical advisers where we seek a report or advice.

Your information may be shared with ABM Group Companies (including ABM Industries Incorporated and its subsidiaries) so that they can provide us with services or if they have a legitimate need for your information.

In certain cases, some of your information may be shared with companies located outside of the United Kingdom, including ABM Industries Incorporated. We will ensure that safeguards are in place to protect your personal information and will only share your information if allowed by law.

Where required by law, we have signed agreements with those organisations or companies we are sharing your data with that are located outside of the United Kingdom. You can receive copies of any agreements that relate to the sharing of your information outside of the United Kingdom by contacting us at UKPrivacyquestions@abm.com.

Your information will only be shared if needed to provide the required services.

What Are Your Rights?

1. You have the right to review, correct and erase your personal data.

You have the right to ask to see any of your personal data that we hold, and to ask for correction of any information that is not correct. You may also ask us to erase information about you that we hold, except for information that we are required to keep by law or that may be needed for legitimate business reasons like processing your pay.

Please visit <https://www.abm.co.uk/gdpr/> to submit a Data Subject Access Request concerning your information.

2. You have the right to receive or transfer your data.

In certain cases, if we have recorded your personal information electronically (such as through a computer), you can ask for a copy of that information or for us to send it to another party.

3. You have the right to limit our use of your information.

You have the right to limit our use of your personal information where:

- you do not agree that the information we have is correct
- where our having or use of the information is unlawful, but you do not want us to erase the information
- where we no longer need your information, but you require it due to a legal claim
- where you object to our having or using the information because of a legitimate interest you have (see section 5 below).

Where we are required to limit our use of your information, we will only use it with your consent or in connection with legal claims.

4. You have the right to withdraw consent.

Where we asked for your consent to collect and use certain information, you can withdraw your consent at any time. You can do this by contacting your HR contact.

5. You have the right to object to us having or using your information on legitimate interest grounds.

Where we are relying on our legitimate interest to collect and use your information, then you have the right to object. If you object, we must stop using your information unless we can either show that we have, (a) a compelling legitimate reason for using your information that overrides your interests, rights, and freedoms or, (b) the need to use your information in connection with a legal claim.

6. You have the right to complain.

If you are employed in the United Kingdom, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) if you consider that the processing of your personal data infringes applicable law (<https://ico.org.uk>). If you are employed in the Republic of Ireland, you may lodge a complaint with the Data Protection Commissioner's Office (<https://www.dataprotection.ie>). For further information regarding your rights, or to exercise any of your rights, please email UKprivacyquestions@abm.com.

Will This Policy Change In The Future?

We may change or update this Employee Privacy Notice at any time.

Should we change certain policies that relate to the collection and use of your information, we will update this Employee Privacy Notice and alert you so that you know which information we collect and use and how long we keep it.

This Employee Privacy Notice was last updated and reviewed on 21st December 2021.